AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF MISSISSIPPI

FILED
Mar 28 2023
ARTHUR JOHNSTON, CLERK

UNITED STATES DISTRICT COURT

for the

Southern District of Mississippi

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
INFORMATION ASSOCIATED WITH [norlanvargas8419@icloud.com] THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.

Case No. 1:23-mj-348-RPM

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, attached hereto and incorporated herein by reference

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
8 USC §§ 1324(a)(1)(A)(ii) & (v)(I) & (B)(i)	Conspiracy to Unlawfully Transport or Move an Alien Within the United States for Commercial Advantage or Private Financial Gain

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Christopher C. Spiers, Border Patrol Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 3-28-2023

Judge's signature

City and state: Gulfport, Mississippi

Robert P. Myers, Jr., U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

Property to be Searched

The property to be searched is described as:

1. Apple iPhone CLOUD account. Furthermore, described as an norlanvargas8419@icloud.com

2. This Apple iPhone CLOUD account has been associated with an electronic device bearing IMEI# 352113531912678 laser etched on the sim card tray, and found in the possession of Javier Norlan Vargas-Bejarano a/k/a Norlan Javier Vargas Bejarano, a/k/a Norlan Javier Bejarano-Vargas, a/k/a Norlan Vargas-Bejarano, a/k/a Norlan Vargas Bejarano, a/k/a Nolan Vargas-Bejarno, a/k/a Noel Jose Vargas. The electronic device currently is in federal custody located at the Gulfport Border Patrol Station located at 10400 Larkin-Smith Drive, Gulfport, MS 39503, in Harrison County, in the Southern Division of the Southern District of Mississippi.

3. The warrant authorizes the forensic examination of the Apple CLOUD account associated to norlanvargas8419@icloud.com.

ATTACHMENT B

Particular Things to be Seized

I. **Information to be disclosed by Apple**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used; and

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, evidence and/or instrumentalities of violations of Title 8, United States Code, Sections 1324(a)(1)(A)(ii) and (v)(I) and (B)(i), Conspiracy to Commit, and the substantive act of Unlawful Transportation or Moving of One or More Aliens within the United States involving Norlan Javier Vargas-Bejarano (and/or aliases/name variations stated in the accompanying affidavit), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____.

I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes).

I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and

c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF MISSISSIPPI

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [norlanvargas8419@icloud.com] THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	**UNDER SEAL** **Case No.** 1:23mj548-RPM

I. INTRODUCTION AND AGENT BACKGROUND

I, Christopher C. Spiers, being first duly sworn state:

1. This Affidavit is submitted in support of a request that the Court issue a warrant for the following Apple Corporation in the United States (hereinafter referred to as Apple) iCloud account norlanvargas8419@icloud.com. This Apple iCloud account has been associated with the IMEI: 352113531912678 and/or one of the following names: Javier Norlan Vargas-Bejarano a/k/a Norlan Javier Vargas Bejarano, a/k/a Norlan Javier Bejarano-Vargas, a/k/a Norlan Vargas-Bejarano, a/k/a Norlan Vargas Bejarano, a/k/a Nolan Vargas-Bejarno, a/k/a Noel Jose Vargas.

2. This affidavit is made in support of an application for a search warrant of the iCloud account norlanvargas8419@icloud.com for information regarding violations of Title 8, United States Code, Sections 1324(a)(1)(A)(ii) & (v)(I) & (B)(i), Conspiracy to Commit, and the substantive act of Unlawful Transportation or Moving of an Alien within the United States. Additionally, search of said iCloud account is for information regarding attempts to conceal evidence of the above-mentioned violations.

3. Your Affiant knows that Apple Corporation in the United States (Apple) is a company that provides free and paid Cloud based storage in connection with their products which can be accessed by the general public. Furthermore, I have learned that stored Cloud data for Apple subscribers, may be located on the computers of Apple. Further, I am aware that computers

located at Apple contain information and other stored electronic communications belonging to unrelated third parties. Accordingly, this affidavit and application for search warrant seeks authorization to seize the records and information specified in Attachment A.

4. Information sought includes data related to videos, pictures, documents, and communications stored in the norlanvargas8419@icloud.com account regarding the Conspiracy to Commit, and the substantive act of Unlawful Transportation or Moving of an Alien within the United States.

5. I am a Border Patrol Agent (BPA) of the United States Border Patrol (USBP), currently located at 10400 Larkin Smith Drive, Gulfport, Mississippi. I am a graduate of the U.S. Border Patrol Academy and have been an Agent in the Border Patrol since on or about February 18, 2013. I have approximately 18 years of experience as a law enforcement officer. As part of my official duties as a BPA, I am authorized and assigned to investigate violations of the immigration laws as well as other criminal statutes of the United States.

6. Your Affiant has become aware of the facts and circumstances described below through my personal observation, my training and experience, information provided by other law enforcement officers and witness interviews. Your Affiant makes this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require Apple Inc., headquartered at Privacy and Law Enforcement Compliance 1 Infinity Loop, Cupertino, California 95014, to disclose to the government records and other information, including the contents of communications, in its possession pertaining to the Apple Corporation iCloud account norlanvargas8419@icloud.com.

II. PERTINENT FEDERAL CRIMINAL STATUTES

7. Title 8, United States Code, Sections 1324(a)(1)(A)(ii) & (v)(I) & (B)(i), Conspiracy to Commit, and the substantive act of Unlawful Transportation or Moving of an Alien within the United States.

III. ACCESS TO STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS

8. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense[s] being investigated." 18 U.S.C. § 2711(3)(A)(i).

9. Accordingly, pursuant to provisions of the Electronic Communications Privacy Act, 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), I seek a warrant to require Apple Inc. to disclose copies of the records and information, including the contents of communications and data storage, described in Section I of Attachment A to this affidavit. Upon receipt of the information described in Section I, authorized law enforcement personnel will review that information to locate the items described in Section II of Attachment A. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of the requested warrant.

IV. BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND APPLE INC.

10. The term "computer" as used herein is defined in Title 18, United States Code, Section 1030(e)(1), and includes "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes

any data storage facility or communications facility directly related to or operating in conjunction with such device…."

11. The Internet is a worldwide network of computer systems operated by, among others, governmental entities, corporations, and universities. In order to access the Internet, an individual computer user generally must subscribe to and/or gain access to an Internet Service Provider (ISP) that operates a host computer system with direct access to the Internet. Every computer or device on the Internet is referenced by a unique Internet Protocol (IP) address the same way every telephone has a unique telephone number. An example of an IP address is 192.168.10.102.

12. The World Wide Web (WWW) is a functionality of the Internet that allows Internet users to share information by means of websites located or stored on different computers around the world. A Universal Resource Locator (URL) is the unique address for a website or file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL (for example, www.ice.gov) of the website's home page file in the web browser's address line. Additionally, any file within that website can be specified with a URL. Websites and files on the Internet may also be accessed by means of their IP addresses. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

13. By accessing the Internet, an individual computer user may communicate or participate in data transfer with millions of computers around the world. An Internet user can connect to the Internet by any number of means, including via modem, local area network, or wireless technology.

14. By registering for an account, an Internet user may use a popular Internet functionality called email. Email permits a user to transmit or receive messages and/or files (including images) to or from other Internet users. Email operates largely through email servers, which are computers on the Internet tasked with performing a specific function, in this case routing electronic mail for a number of users. Typically, a user addresses and composes an email on his computer or on a website (for example, www.yahoo.com) provided for that purpose by his email service provider. When the user clicks send, the message is sent to the user's email provider's mail server, which routes it from there through several intermediate computers to the addressee's email provider's mail server, which ultimately delivers it to the addressee. The addressee may then read the email on his computer or on a website provided for that purpose by his email provider.

15. An email to or from a user may be saved by that user's email provider either at the user's request or as a function of the provider's service. In addition, the provider may retain information and records regarding its customers and the usage of any email accounts or other provided services.

16. Apple Inc., an electronic communication, data storage service and remote computing service, provides, among other things, free and paid data storage services to the public. Users can obtain a free iCloud account using an email account by registering with Apple and providing unverified basic information including the subscriber's name and other information. The information provided is not authenticated by Apple Inc. Some subscribers may choose to pay a fee for enhanced services.

17. Apple Inc. maintains electronic records pertaining to the individuals and companies for which it maintains subscriber accounts. In addition to the information described above, these

records include account access information, data storage information, and account registration information. This information may include the date on which the account was created, the length of service, records of log-in or session times and durations, the types of services utilized, the status of the account, the methods used to connect to the account, records of the Internet Protocol address used to register and to log into the account, and other log files that reflect usage of the account and other services. In some cases, iCloud account users will communicate directly with a service provider like Apple Inc. about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers like Apple Inc. typically retain records about such communications, including records of any actions taken by the provider or user as a result of the communications.

18. Generally, Apple Inc. iCloud subscribers access their accounts using their phone or through a web interface. To use Apple Inc. iCloud services, subscribers are required to secure access to the Internet via some other Internet or telecommunications service provider. Apple Inc. iCloud subscribers can access the service from anywhere in the world, provided that they are able to secure this Internet access. When a subscriber connects to Apple Inc. iCloud, the subscriber is required to provide an identity, through a username, and to authenticate this identity by providing a password. Once a subscriber is successfully authenticated, Apple Inc. creates a record of the connection (listing, for example, the Internet Protocol address connected from and the date and time of the connection).

19. An Apple Inc. iCloud subscriber may store email, chat logs, contact lists reflecting individuals/contacts with whom the subscriber corresponds, calendar data, pictures, videos, and other files on servers maintained and/or owned by Apple Inc. In my training and experience,

evidence of who used an email account may be found in address books, contact lists, emails in the account, and attachments to emails, including pictures and files.

20. A subscriber may store email and other such files and records on Apple Inc. iCloud's servers for reasons of convenience or due to the lack of storage space on the subscriber's own computer or communications device. If a subscriber does not delete an email message or other stored file, the data may remain on Apple Inc. iCloud's servers indefinitely. Even if a subscriber deletes account data on his or her phone, computer, or device, it may continue to be available on Apple Inc. iCloud's servers for a certain period of time. For that reason, a search of a subscriber's phone or "home" computer will not necessarily uncover the records, files, messages, and other information maintained by a subscriber on Apple Inc. iCloud's servers.

V. PROBABLE CAUSE

Summary

21. On or about November 9, 2022, at approximately 9:30 pm, a Deputy with the Harrison County Sheriff's Department Criminal Interdiction Patrol (CIP), contacted the United States Border Patrol (USBP) Gulfport Station (GPS) concerning a vehicle stop at the 31 mile marker on I-10 east. The Deputy stopped a black 2016 Toyota Highlander with a certain temporary Texas tag for careless driving.

22. The driver identified himself with a Maryland driver's license as Norlan Javier Vargas-Bejarano, residing in Silver Spring, Maryland. Vargas-Bejarano claimed he and all passengers were traveling to work in Miami, Florida. The deputy observed no visible luggage or tools indicating the passengers intended to immediately work upon arrival. He also noticed bottled water, fast food bags and several caffeinated drink cans throughout the vehicle. Due to

the deputy's experience and training, he recognized the driver may be involved in criminal alien smuggling and contacted Border Patrol.

23. USBP Agents arrived on scene and questioned the driver and passengers as to their citizenship. The driver and passengers were determined to be illegally in the United States without proper documentation and were transported to the USBP Gulfport Station for further processing.

24. At the Gulfport Border Station, Vargas-Bejarano was processed using the e3/IDENT and IAFIS electronic systems. His fingerprints were electronically scanned and were automatically matched by computer to his fingerprints in prior immigration records. His identity as Norlan Javier Vargas-Bejarano, was positively confirmed based on records checks received from computerized fingerprint analysis and visual analysis of prior immigration photographs of Vargas-Bejarano.

25. Official Record checks revealed that Vargas-Bejarano was initially encountered on or about May 24, 2003. He was processed for an Expedited Removal, was ordered removed on or about May 24, 2003, and was physically deported or removed from the United States to his native country of Honduras on or about August 7, 2003, via in or near Houston, Texas. Vargas-Bejarano claimed to have illegally re-enter the United States on foot through Laredo, Texas in 2008. Vargas-Bejarano stated he has been living in the United States ever since.

26. During a Post-Miranda video-recorded interview, Vargas-Bejarano stated he is currently living with a friend in Houston, Texas named Frazzie. He was unable to provide an address, although claimed to live with her for six weeks. Vargas-Bejarano stated he met the passengers when they "arrived" at Frazzie's two days ago. Vargas-Bejarano claimed one of the passengers made arrangements for everyone to work in Miami, Florida and he would take them

there. Vargas-Bejarano claimed he paid for gas and the passengers paid for their own food along the way. Vargas-Bejarano hoped the passengers would repay him for the gas after finding work in Miami. Vargas-Bejarano did admit he knew all passengers were illegally present in the United States.

27. During the questioning of the five passengers, Ana Gabriela AVILA-Ramirez, Lorenzo ESPINDOLA-Angeles, Eber Guadencio ORTEGA-Guzman, Jonatan Natanael ALVAREZ-Martinez and Alfonso Frederico ALVAREZ-Martinez. AVILA admitted that she was to pay Vargas-Bejarano $1,500.00 to be transported to Virginia. ESPINDOLA admitted that he was pay Vargas-Bejarano $800.00 to be transported to South Carolina. ORTEGA admitted that he was to pay Vargas-Bejarano $800.00 to be transported to Florida. ALVAREZ admitted that he was to pay Vargas-Bejarano $1,500.00 to be transported to Florida. ALVAREZ admitted that he was to pay Vargas-Bejarano $1,500.00 to be transported to Florida.

28. Vargas-Bejarano was found in possession of $8,440.00. Vargas-Bejarano claimed it was money he has saved as a result of working in Texas. Vargas-Bejarano was asked if he had a bank account and debit card and which he replied yes. Vargas-Bejarano was asked why he did not keep his money in his account and Vargas-Bejarano could not answer the question. The $8,440.00 is believed to be proceeds from criminal alien smuggling and is being seized by USBP.

29. On or about December 5, 2022, an application for a search warrant was applied for a granted. The search warrant was for an Apple iPhone cellular device belonging to Vargas-Bejarano. The Apple iPhone was turned over HSI Special Agent and Forensic Analyst Troy McCarter for download and analysis. During the download it was determined that the Apple iPhone was inaccessible due to the model and age of the phone.

30. On or about December 15, 2022, BPA Spiers contacted the Department of Justice (DOJ) Computer Crime and Intellectual Property Section (CCIPS) for assistance. It was determined that the Apple iPhone CLOUD is possibly still accessible thru Apple databases.

31. On or about January 3, 2023, BPA Spiers contacted Apple Law Enforcement via email. The email included a signed search warrant for pertaining to IMEI# 352113531912678. This IMEI# was located on sim tray card belonging to a phone possessed by Vargas-Bejarano.

32. On or about January 10, 2023, Apple Law Enforcement responded back with an email containing documents pertaining to IMEI# 352113531912678 and the associated icloud account norlanvargas8419@icloud.com.

33. Based on my training, experience, and knowledge, and information provided to me by other agents who specialize in computer forensics, I know the following:

a) The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. In order to access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web ("www") is a functionality of the Internet which allows users of the Internet to share information;

b) With a computer connected to the Internet, an individual computer user can make electronic contact with other computers around the world. This connection can be made by any number of means, including modem, local area network, wireless, and numerous other methods;

c) iCloud is a popular form of data storage in an electronic environment. When an individual phone or computer user uploads data the receiving server is a computer that is attached to a dedicated network and serves many users. An iCloud server may allow users to view/upload/download/modify via electronic means.

34. Based on my training, experience, and knowledge, and information provided to me by other agents who specialize in computer forensics, I have learned the following about Apple:

a) Apple subscribers obtain an account by registering an email account with Apple. Apple requests subscribers to provide basic information, such as name, gender, zip code and

other personal/biographical information. This information is not verified and is based upon the information provided by the subscriber. Apple obtains payment information (credit card number, bank account number) for the paid account services;

b) Apple maintains electronic records pertaining to the individuals and companies for which it maintains subscriber accounts. These records include account access information, iCloud uploads/downloads/views/modifications/deletions, and account application information;

c) Subscribers to Apple may access their accounts on servers maintained, leased and/or owned by Apple from any computer connected to the Internet located anywhere in the world;

d) When the subscriber uploads to the iCloud, it is initiated by the user at the user's phone or computer and transferred via the Internet to Apple servers where the information is stored. Apple users have the ability to manage the data they store on the iCloud which includes the ability to view/upload/download/modify data stored therein, on servers maintained, leased and/or owned by Apple.

35. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Apple, to protect the rights of the subject of the investigation, and to effectively pursue this investigation, authority is sought to allow Apple to make a digital copy of the entire contents of the information subject to seizure specified in Attachment A. That copy will be provided to your Affiant or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Attachment A.

36. On January 3, 2023, the Affiant submitted a preservation request for records and other information, including the contents of communications, in its possession pertaining to the Apple Corporation iCloud subscriber using the IMEI 352113531912678 or name Javier Norlan VARGAS-Bejarano. Apple Corporation responded to the Affiant acknowledging receipt of

preservation request and pursuant to 18 U.S.C. § 2703(f), available data will be preserved for 90 days.

VI. CONCLUSION

37. Based on the foregoing, there is probable cause to believe that the iCloud account connected to the norlanvargas8419@icloud.com accounts identified in Attachment A has been used in the commission of a crime and constitute evidence, fruits, and instrumentalities of violations of federal laws of the United States. These violations specifically include violations of Title 8, United States Code, Sections 1324(a)(1)(A)(ii) and (v)(I) and (B)(i), Conspiracy to Commit, and the substantive act of Unlawful Transportation or Moving of One or More Aliens within the United States.

Christopher C. Spiers
Border Patrol Agent
United States Border Patrol

Sworn and subscribed to before me
this 28th day of March 2023.

Robert P. Myers, Jr.
United States Magistrate Judge

ATTACHMENT A

Property to be Searched

The property to be searched is described as:

1. Apple iPhone CLOUD account. Furthermore, described as an norlanvargas8419@icloud.com

2. This Apple iPhone CLOUD account has been associated with an electronic device bearing IMEI# 352113531912678 laser etched on the sim card tray, and found in the possession of Javier Norlan Vargas-Bejarano a/k/a Norlan Javier Vargas Bejarano, a/k/a Norlan Javier Bejarano-Vargas, a/k/a Norlan Vargas-Bejarano, a/k/a Norlan Vargas Bejarano, a/k/a Nolan Vargas-Bejarno, a/k/a Noel Jose Vargas. The electronic device currently is in federal custody located at the Gulfport Border Patrol Station located at 10400 Larkin-Smith Drive, Gulfport, MS 39503, in Harrison County, in the Southern Division of the Southern District of Mississippi.

3. The warrant authorizes the forensic examination of the Apple CLOUD account associated to norlanvargas8419@icloud.com.

ATTACHMENT B

Particular Things to be Seized

I. **Information to be disclosed by Apple**

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWorks (including Pages, Numbers, and Keynote), iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

g. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

h. All records pertaining to the types of service used; and

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes contraband, evidence and/or instrumentalities of violations of Title 8, United States Code, Sections 1324(a)(1)(A)(ii) and (v)(I) and (B)(i), Conspiracy to Commit, and the substantive act of Unlawful Transportation or Moving of One or More Aliens within the United States involving Norlan Javier Vargas-Bejarano (and/or aliases/name variations stated in the accompanying affidavit), including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);

b. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

c. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

d. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

e. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Apple Inc., and my official title is _____.

I am a custodian of records for Apple Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Apple Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes).

I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Apple Inc.; and

c. such records were made by Apple Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature